

Computer Viruses

A computer virus is a small program that attaches itself to another program and attacks other software by making copies of itself.

Lecture Plan

- What is a Computer Virus?
- Types of Computer Viruses
- Famous Viruses
- Virus Protection Strategies through practice of safe computing
- Virus Protection Software
- What Virus Protection Should We Use in Enterprise Network?

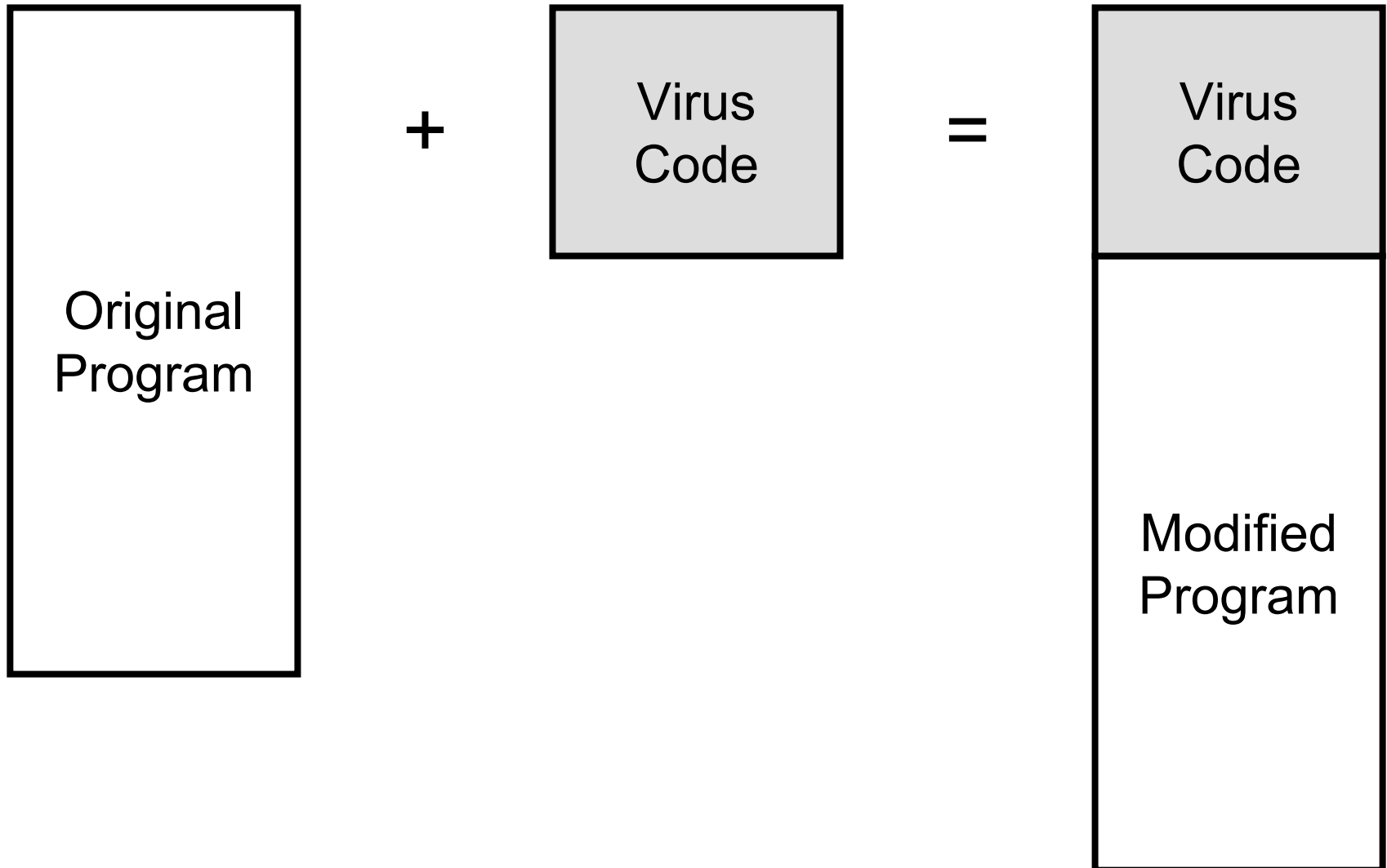
What is a Computer Virus?

- **Computer Virus** - The term was first used by Fred Cohen in 1984.
- A computer virus is a small program that attaches itself to another program and attacks other software by making copies of itself.
- A virus executes when an infected program is executed. Therefore only executable files can be infected.

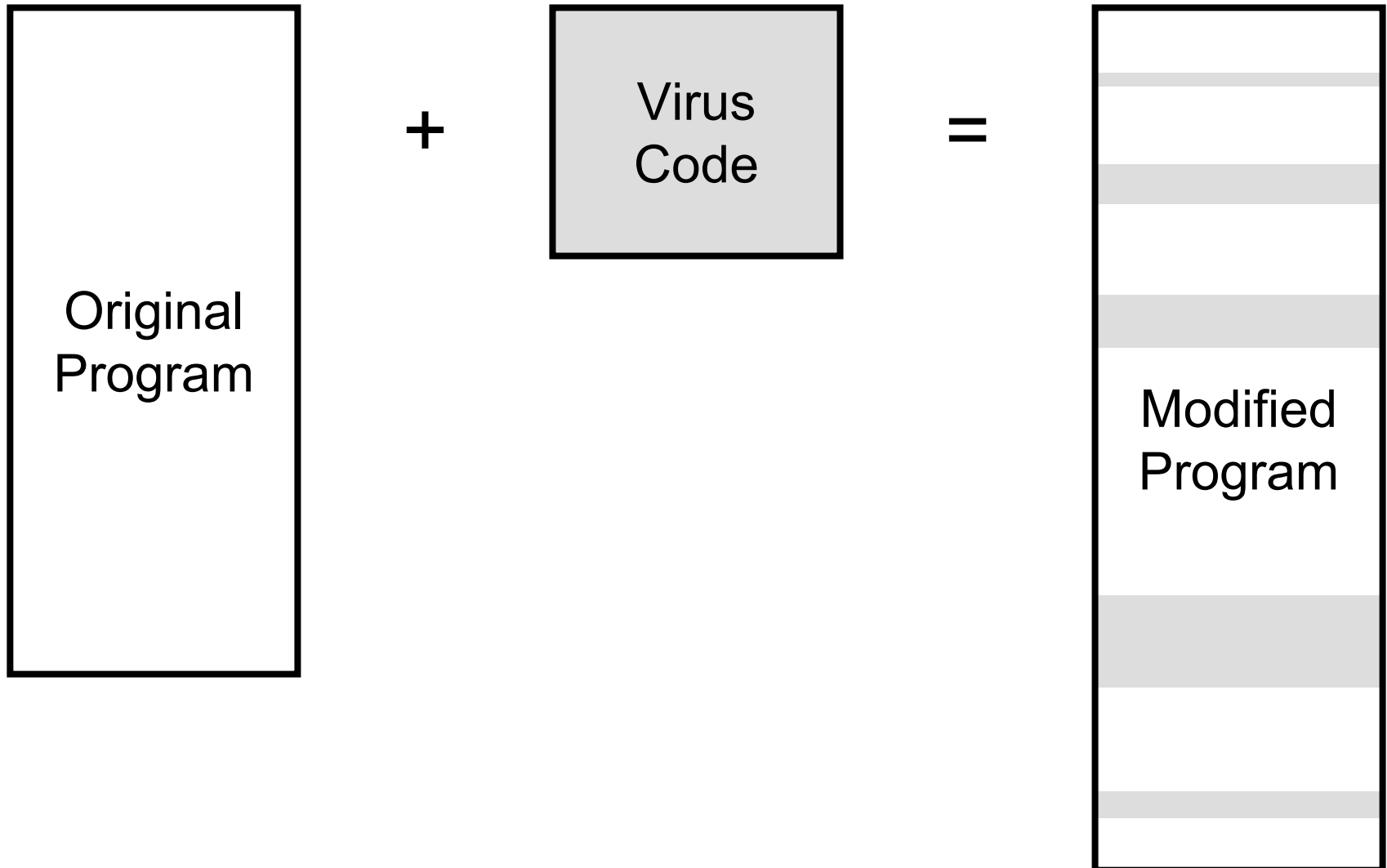
Computer Viruses are Small

- Virus programs, like the infectious microorganisms that are their namesakes, are often small.
- Only a few lines of program code are required to write a simple virus.
- The implication is clear: viruses can be easily hidden in healthy software and therefore prove very difficult to find.

Viruses attach to programs



Viruses can be easily hidden in healthy software



Who Do Computer Viruses Infect and How?

- Viruses can infect any computer, from a small laptop to a multi-million dollar mainframe.
- Anyone who owns a personal computer can create a virus program. This means virus development tools are widely available.
- Once written, a virus can be transmitted over telephone lines or distributed on infected disks to other systems, where it can reproduce in microseconds to damage the biggest systems thousands of miles away.
- These two facts make it virtually impossible to trace any virus back to the person who originally wrote it.

Destructive Non-Virus Programs

- Aside from viruses, there are other threats to user systems, including:
 - ⊗ Worms
 - ⊗ Trojan Horses
 - ⊗ Logic Bombs
- As well as being potentially destructive by themselves, each can also be used as a vehicle to propagate any virus.

Worms

- Worm - A worm is a program (usually stand-alone) that worms its way through either the computer's memory or a disk and alters data that it accesses.
- It is different from a computer virus since it does not require a host.

Worms

- Worms are constructed to infiltrate legitimate data processing programs and alter or destroy the data. Often what people believe is a virus infection is, in fact, a worm program. This is not as serious because worms do not replicate themselves. But the damage caused by a worm attack can be just as serious as a virus, especially if not discovered in time. For example, suppose a worm program instructs a bank's computer to transfer funds to an illicit account. The fund transfers may continue even after the worm is destroyed. However, once the worm invasion is discovered, recovery is much easier because there is only a single copy of the worm program to destroy since the replicating ability of the virus is absent. This capability may enable it to re-infect a system several times. A worm is similar to a benign tumor while a virus is like a malignant one.

Trojan Horses

- Trojan horse - A program which attaches itself to a seemingly innocent program.
- A Trojan Horse is a destructive program that has been disguised (or concealed in) an innocuous piece of software.
- Worm and virus programs may be concealed within a Trojan Horse.
- Trojan horses do not necessarily replicate - Trojan Horses are not viruses because they do not reproduce themselves and spread as viruses do.

Trojan Horses

- The mythical story of the original Trojan Horse is well known. When Greek warriors concealed themselves in an attractive wooden horse and left it outside the gates of the besieged city of Troy, the Trojans assumed it was a friendly peace offering and took it in. The Greek warriors then leaped out and wreaked havoc. Trojan Horse software works on the same principle. A program may seem both attractive and innocent, inviting the computer user to copy (or download) the software and run it. Trojan Horses may be games or some other software that the victim will be tempted to try.

Logic Bombs / Time Bomb

- Logic or time bomb - A program that is activated or triggered after or during a certain event.
- This may be after several executions or on a certain day like Friday the 13th.

Logic Bombs

- Writing a logic bomb program is similar to creating a Trojan Horse. Both also have about the same ability to damage data, too. Logic bombs include a timing device so it will go off at a particular date and time.
- The Michelangelo virus is embedded in a logic bomb, for example. Other virus programs often include coding similar to that used in logic bombs, but the bombs can be very destructive on their own, even if they lack the ability of the virus to reproduce. One logic bomb caused major problems in the Los Angeles water department's system. (or download) the software and run it.

Logic Bombs

- Logic bombs are usually timed to do maximum damage. That means the logic bomb is a favored device for revenge by disgruntled former employees who can set it to activate after they have left the company. One common trigger occurs when the dismissed employee's name is deleted from payroll records. On one occasion, a student left a logic bomb timed to explode and wipe out his university's records well after he had collected his degree and was long gone. This example illustrates the pernicious nature of logic bombs which can be written literally decades before they explode.

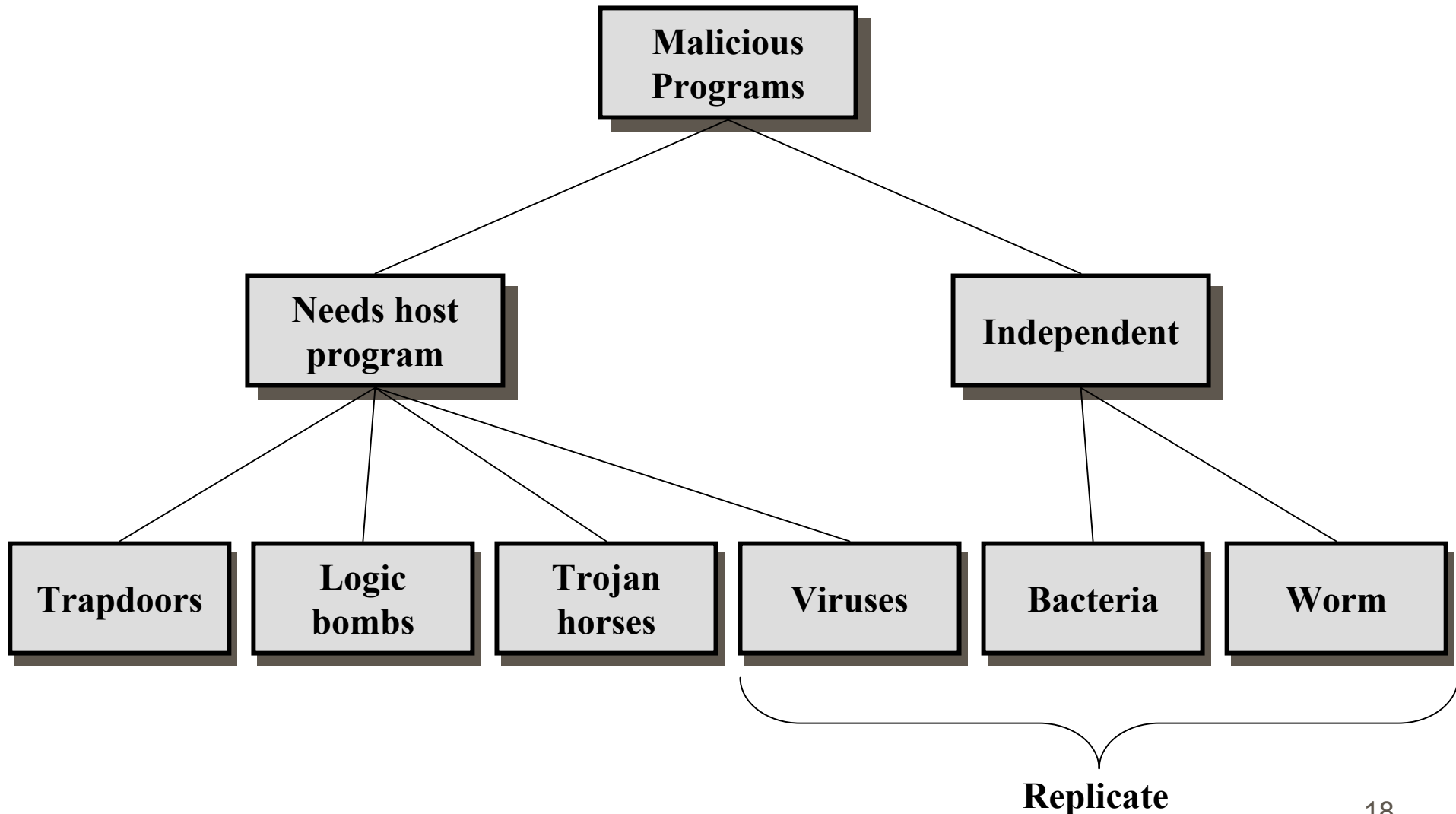
Rabbit

- A program that replicates itself without limit to exhaust a resource.
- For example a program that keeps on making copies of itself on the hard disk till no hard disk space is left.
- Or a program that keeps loading instances of itself in the memory till all available memory is exhausted and the system is unable to perform due to unavailability of free memory.
- Rabbits are also called **bacteria**.

Summary of Malicious Code

Code Type	Characteristics
Virus	Attaches itself to program and propagates copies of itself to other programs
Trojan horse	Contains unexpected, additional functionality
Logic bomb	Triggers action when condition occurs
Time bomb	Triggers action when specified time occurs
Trapdoor	Allows unauthorized access to functionality
Worm	Propagates copies of itself through a network
Rabbit	Replicates itself without limit to exhaust a resource

Summary of Malicious Code



Types of Viruses

- There are several different types of viruses that can infect PC systems, including:
 - ⊗ Boot sector viruses
 - ⊗ File infecting viruses
 - ⊗ Polymorphic viruses
 - ⊗ Stealth viruses
 - ⊗ Multi-partite viruses
 - ⊗ Macro Viruses

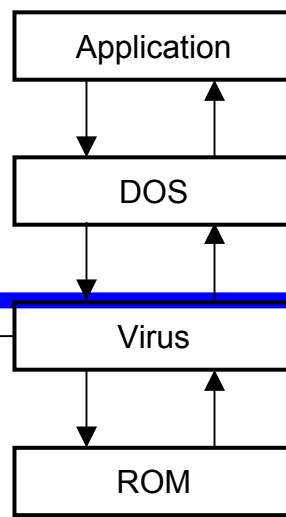
Types of Viruses

- Boot sector infector - hides in the boot sector of a disk or the partition table of a hard disk and takes over control of the computer system when it is booted.
- It then copies itself into the computer's memory.
- When other disks are used, the virus transfers to their boot sectors.
- The most common boot sector viruses were, at one time, the Pakistani Brain virus and the Stoned/Marijuana virus.

Boot Sector Viruses

- Boot sector viruses are those that infect the boot sector (or master boot record) on a computer system. They first move or overwrite the original boot code, replacing it with infected boot code. They will then move the original boot sector information to another sector on the disk, marking that sector as a bad spot on the disk so it will not be used in the future. Boot sector viruses can be very difficult to detect since the boot sector is the first thing loaded when a computer is starts. In effect, the virus takes full control of the infected computer.

The Boot Virus Infection Process

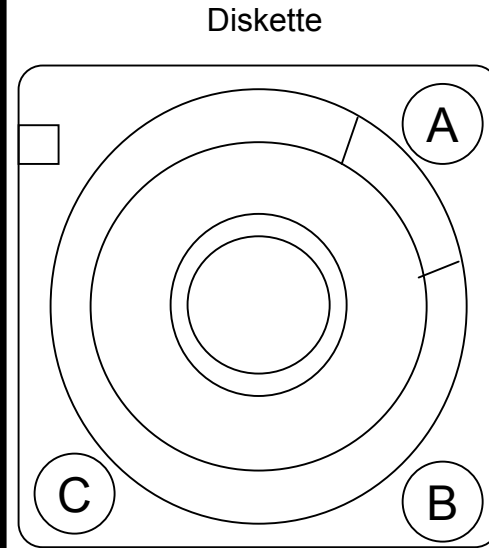
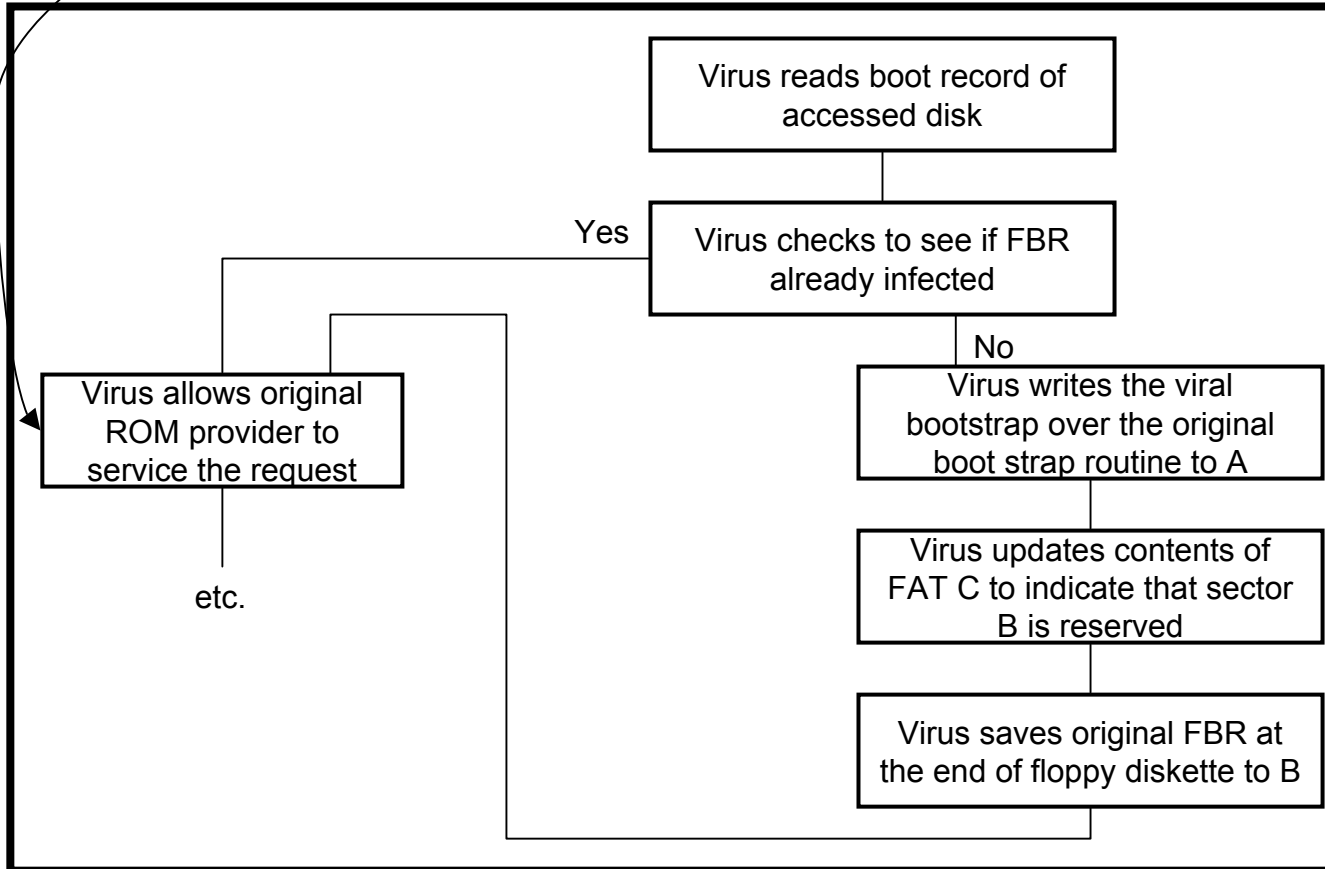


1

Application makes request to access floppy diskette to DOS

2

DOS calls what it thinks is the BIOS diskette service provider to read or write the contents of the floppy diskette. It actually calls the virus.



Types of Viruses

- Application program infector - The most infectious type of computer viruses is the application program infector or file virus. They may attach to any executable file usually .COM and .EXE files. An application program infector takes control after the initial use of the infected program. Once the virus is in place in the RAM of the computer system, it will potentially infect every program run on the computer until the computer is shut off. The most widespread such virus at one time was the Jerusalem virus.

Types of Viruses

- Stealth viruses - viruses which attempt to hide their presence. Some of the simple techniques include hiding the change in date and time and hiding the increase in file size. Some even prevent anti-virus software from reading the part of the file where the virus is located. Some also encrypt the virus code using variable encryption techniques.

Stealth Viruses

- Stealth viruses attempt to hide from both the operating system and anti-virus software. To do this, they must stay in memory so they can intercept all attempts to use the operating system (system calls). The virus can hide changes it makes to file sizes, directory structures, and/or other operating system aspects. Since part of the virus is memory resident, there will be less memory available to users. The virus must hide this fact as well as from both users and anti-virus software. Stealth viruses must be detected while they are in memory. Once found, they must be disabled in memory before the disk-based components can be corrected.

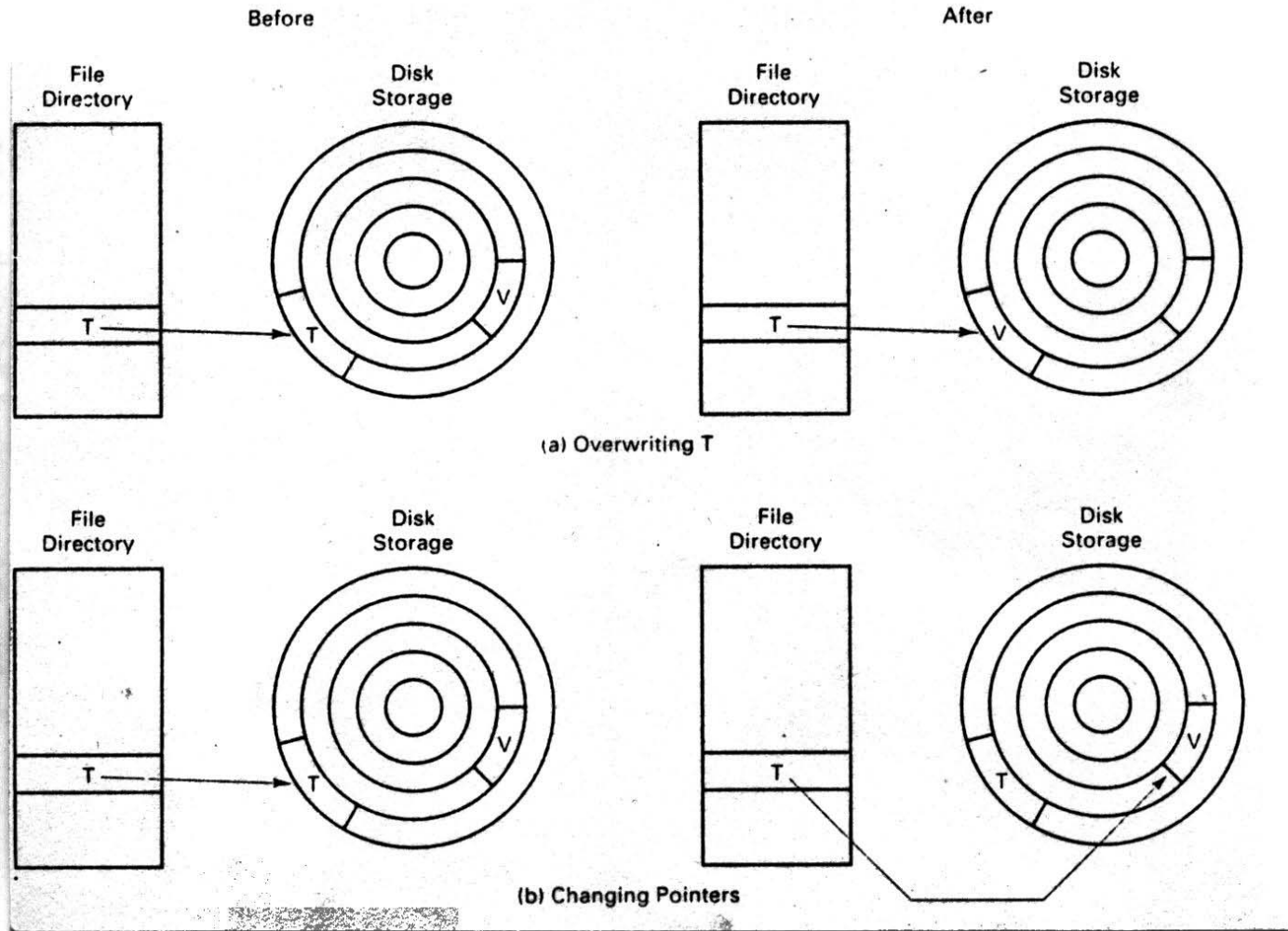
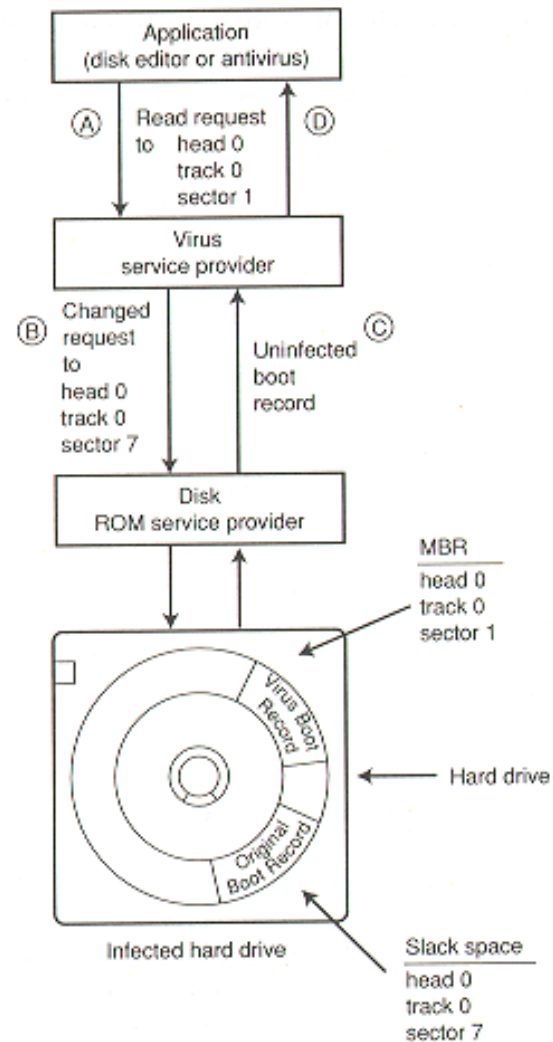


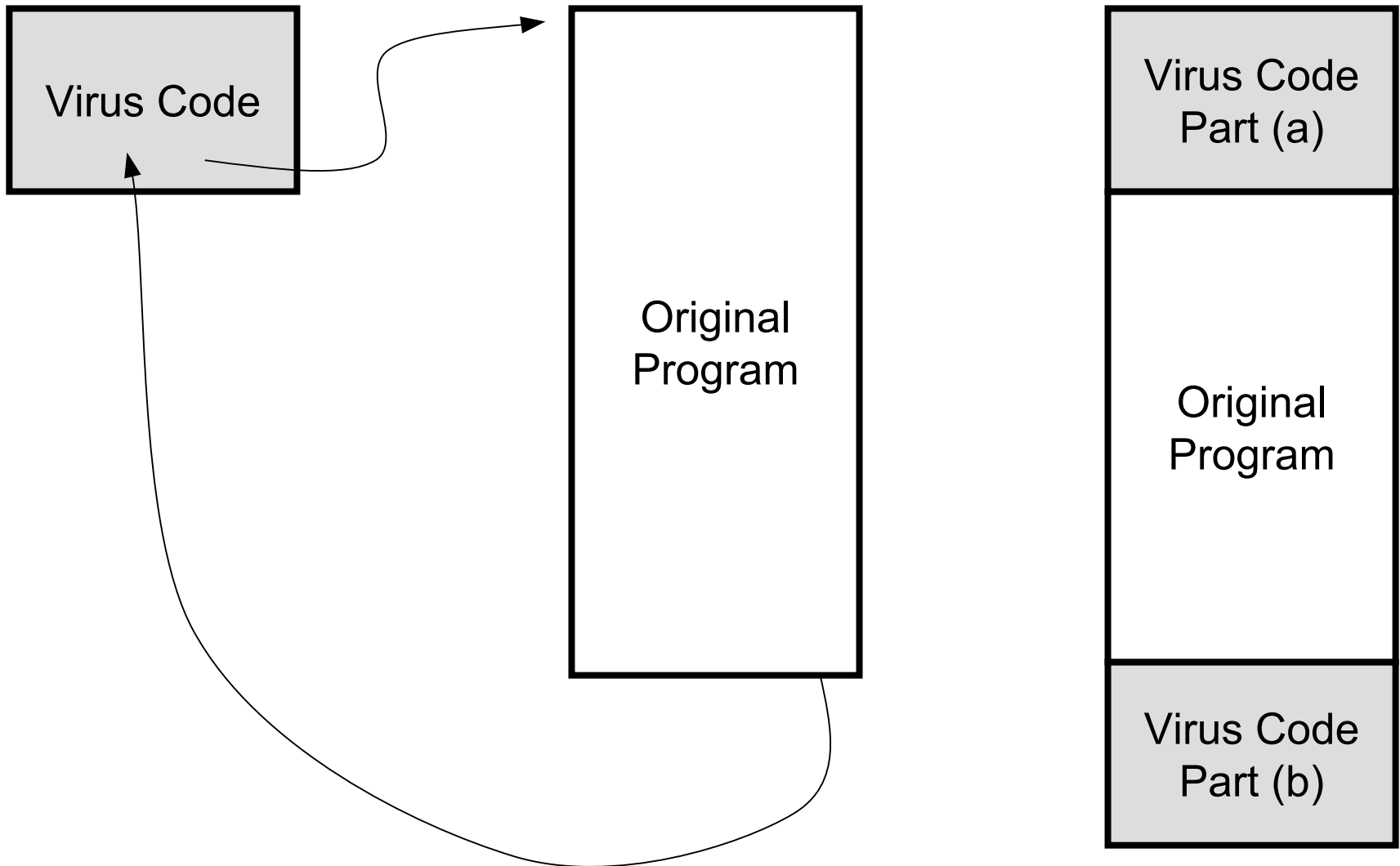
Figure 15.31
Operation of a stealth MBR virus.



- (A) Application requests a read of the boot record of floppy diskette.
- (B) Virus service provider intercepts request (realizing that the application is trying to read the viral boot record). Virus changes request to retrieve the original boot record from track 0, head 0, sector 7.
- (C) and (D) ROM service provider provides the original boot record data to the application.

Physically

Logically



Polymorphic Viruses

- Polymorphic viruses change their appearance with each infection. Such encrypted viruses are usually difficult to detect because they are better at hiding themselves from anti-virus software. That is the purpose of the encryption.
- Dark Avenger Mutation Engine - polymorphic encryption program used by virus developers to encrypt the virus in order to avoid detection. The engine uses a special algorithm to generate a completely variable decryption routine each time. No three bytes remain constant from one sample to the next.

Polymorphic Viruses

- Polymorphic viruses take encryption a step further by altering the encryption algorithm with each new infection.
- Some polymorphic viruses can assume over two billion different guises. This means anti-virus software products must perform algorithmic scanning, as opposed to standard string-based scanning techniques that can find simpler viruses.

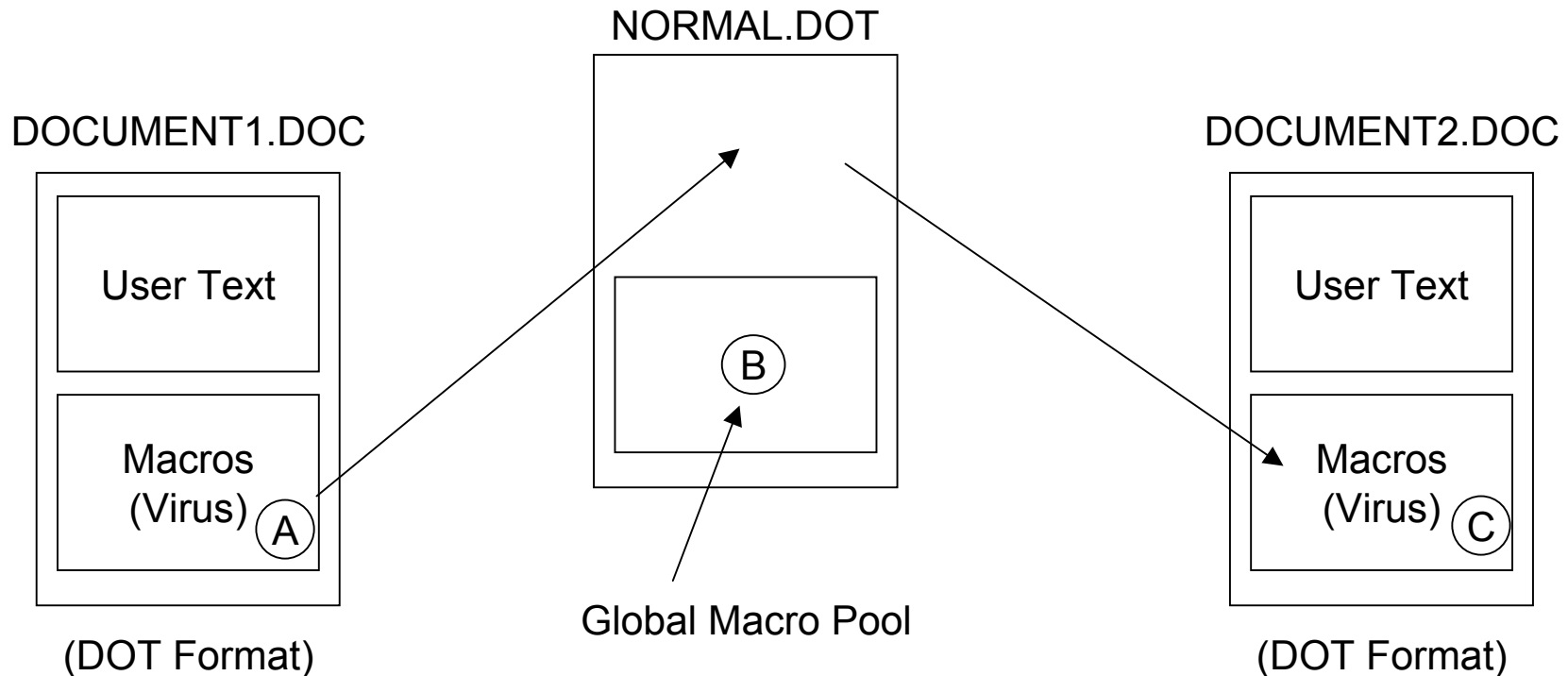
Types of Viruses

- Multiparite virus - virus which infects both the boot sector of a disk as well as application programs.
- Multi-partite viruses are the worst viruses of all because they can combine some or all of the stealth techniques, along with polymorphism to prevent detection.

Types of Viruses

- Macro viruses - virus which attaches to a wordprocessing or spreadsheet file (typically a MS Word or Excel file) as a macro. Once the file is accessed, it replaces one of the Word or Excel standard macros with an infected version which can then infect all subsequent documents.

Macro Virus Propagation



- (A) Macro viruses are stored in the local pool of DOCUMENT1.DOC
- (B) Macro viruses are copied to the global pool (e.g., NORMAL.DOT)
- (C) Virus macros copied from global pool to local pool of document2. Document2 must be converted to DOT format when saved

Examples of Viruses

- Pakistani Brain virus - a boot sector virus that transfers the current boot sector to an unused portion of the disk and marks that portion of the disk as bad sectors. The virus then copies the remainder of the virus to an unused portion of the disk and marks that portion as bad sectors also. The Brain virus then periodically marks other portions of the disk as bad sectors making files and eventually the disk unusable. Early versions displayed a volume label (c) Brain. All versions have the name of the program, the authors and often their address in the boot sector of the infected disk. This virus was the first virus known to spread worldwide and has spawned numerous strains of similar viruses including the Ashar or Ashar-Shoe virus, which became very widespread in Malaysia.

Examples of Viruses

- Stoned-Marijuana virus - is also a boot sector virus. It infects the boot sector of floppy disks and the File Allocation Table (FAT) of hard disk systems. On most systems it will only periodically display a message "Your PC is Stoned. Legalise Marijuana." However on hard disk systems with more than one partition and on floppy disks that have been formatted high density, it will damage the file allocation table. This makes access to the files nearly impossible. The original strain of this virus was written in New Zealand.

Examples of Viruses

- Jerusalem virus - also known as the Israeli and Friday 13th virus and includes several strains including the Jerusalem-B virus. The Jerusalem virus infects both .COM and .EXE files. This virus will survive a warm boot. After the virus is resident for 1/2 hour, it slows the system down by a factor of ten. On Friday the 13th, it will delete all infected files. Besides the damage it inflicts, the Jerusalem-B virus also periodically displays a "black window" in the middle of the screen.

Examples of Viruses

- Cascade virus - also known as the Falling Letters or 1701 virus. It originally appeared as a Trojan Horse disguised as a program to turn off the Num-Lock light. Instead it caused all the characters on the screen to fall into a pile at the bottom of the screen. It now occurs as a memory resident .COM virus. The Cascade virus uses an encryption algorithm to avoid detection. It originally activated on any machine with a color monitor in September-December in the years 1980 and 1988.

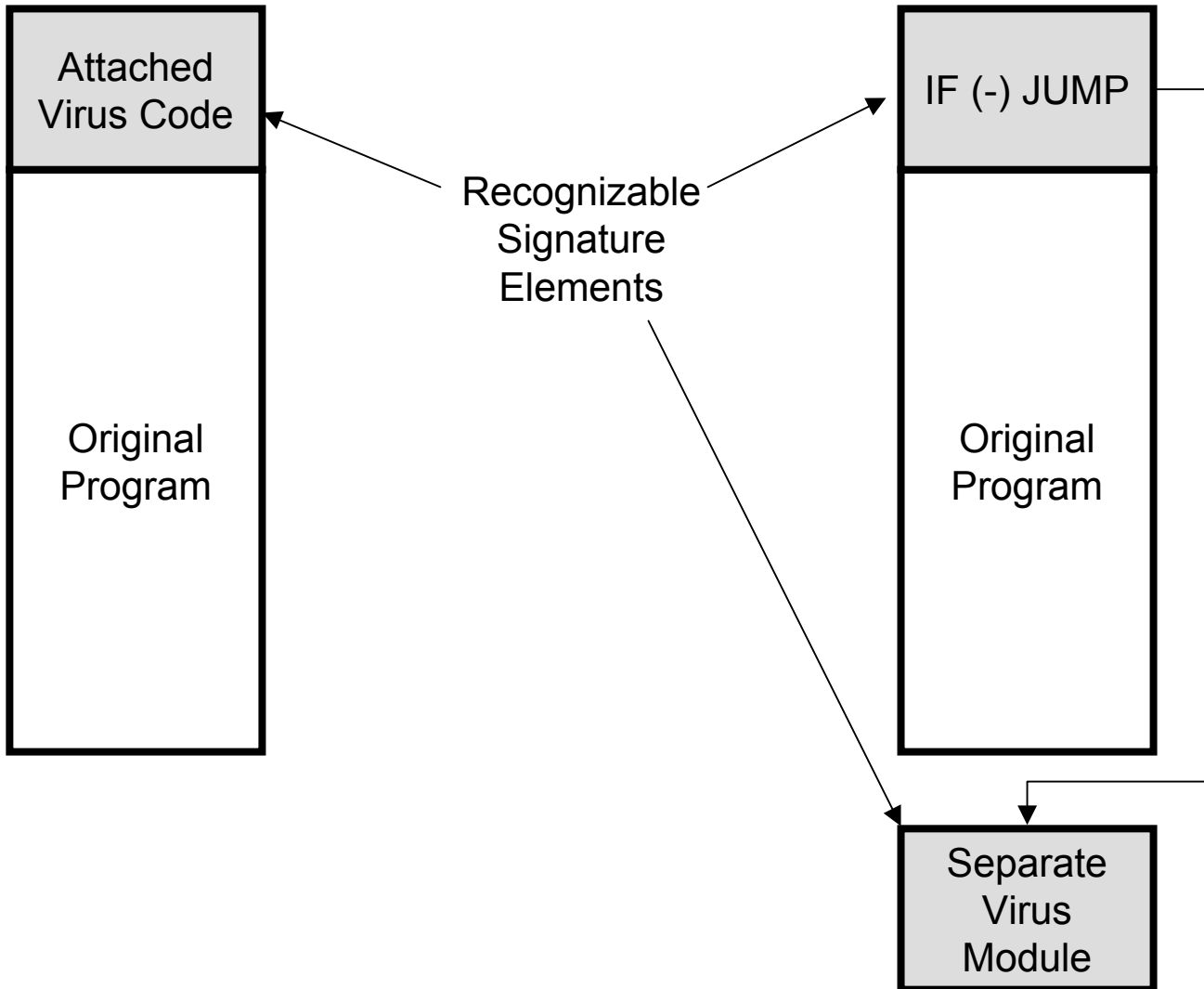
Examples of Viruses

- Michelangelo - on March 6th, if the infected computer is a '286 or '386 computer, the virus will write garbage on all tracks of all cylinders.
- Black Monday - on Mondays, a counter counts down from 240 each time a file is infected. When zero is reached, a low level format of the hard disk is performed. Written by a Malaysian student.

More Recent Viruses

- Nimda
- Code Red
- Worms + Viruses
- Trojans + Trap Doors
- Viruses spreading through email (scripts in emails)

Virus Detection Software Uses Virus Signatures



Do's and Don't's of Safe Computing

- **The spread of computer virus infections can be stopped through the practice of "safe computing."**
- **The following are a list of do's and don't's for safe computing.**

Do's and Don't's of Safe Computing

- 1. Don't use illegal software! If the software has been obtained illegally, how can you assume that it doesn't contain a virus.
- 2. Never boot your computer system from a diskette other than the original DOS diskette. Only one write-protected boot disk should be assigned to a floppy-based system. The diskette should be clearly marked, write-protected and used only for booting up the designated computer. If you accidentally try to boot from a non-system disk, turn the computer off and boot with the write-protected system disk.

Do's and Don't's of Safe Computing

- 3. If your system uses a fixed disk, never boot from a diskette. In some situations, write protection software for the hard disk should be employed.
- 4. Always write-protect your systems and program disks. Write-protect tabs are easy to use and very effective. You should write only on data disks.
- 5. Only copy files from the original distribution disks.

Do's and Don't's of Safe Computing

- 6. Always keep at least one set of back-up copies of all original disks. (This won't prevent a virus infection, but it will help in the recovery process if an infection occurs.)
- 7. Do not loan out program disks. They may be infected when they are returned. If you must loan a disk, always check it for viruses or format it before using the disk on your computer system.

Do's and Don't's of Safe Computing

- 8. Never use a computer that has already been turned on by another user. Always use a cold boot to restart the computer. Do not assume that a warm boot will remove a virus.
- 9. Make all the .COM and .EXE system and program files read only by using the command ATTRIB+R. Some viruses can now circumvent this method.

Do's and Don't's of Safe Computing

- 10. Always keep a lookout for strange occurrences:
 - a. When you do a directory listing, look at the volume label.
 - b. Observe whether your computer system is slowing down.
 - c. Watch for files that disappear.
 - d. Notice when there are attempts to access the disks when there should not be any read or write activity.
 - e. Watch whether the loading of programs takes longer.
 - f. Keep a lookout for decreases in the main memory or reduction of disk space.
 - g. Watch for unusually large sizes on program files.
 - h. Watch for recent creation dates on old program files.
 - i. Watch for unusual displays on the computer screen.

Do's and Don't's of Safe Computing

- 11. Use caution when using public domain and shareware software or any new software. There have been instances where commercial software has been sold with a virus.
- 12. If you are downloading software from a bulletin board or other computer network including the Internet, always download to a diskette. You should then scan the diskette for possible virus infections. (You may want to write-protect your hard disk during this operation.)

Do's and Don't's of Safe Computing

- 13. In a lab environment, do not allow users to run their own programs or boot the computer system with their own disks. Users should only have data disks that are not bootable. All program disks and hard disks in a lab must be checked frequently for viruses. If users are allowed to use their own program disks, they must be scanned before they are used in the computer lab.
- 14. Most important of all is to teach computer users about computer viruses so that they can recognize them. Computer users need to be able to identify viruses so that they will be able to prevent their spread

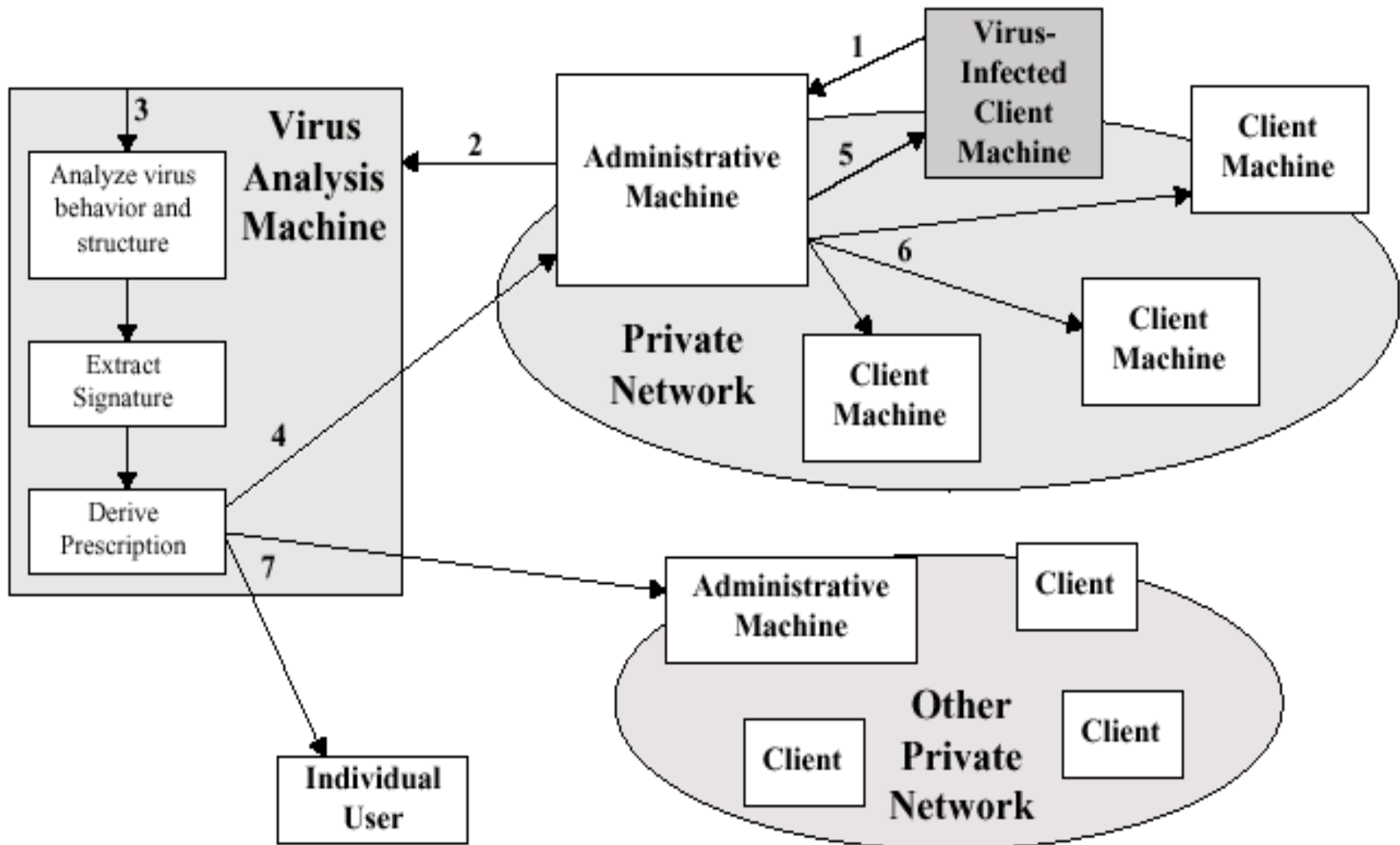
Virus Protection Software

- Norton Antivirus
- McAfee Virus Scan, NetShield
- Cheyenne Innoculan
- Dr. Solomon's Antivirus Toolkt
- Many Others

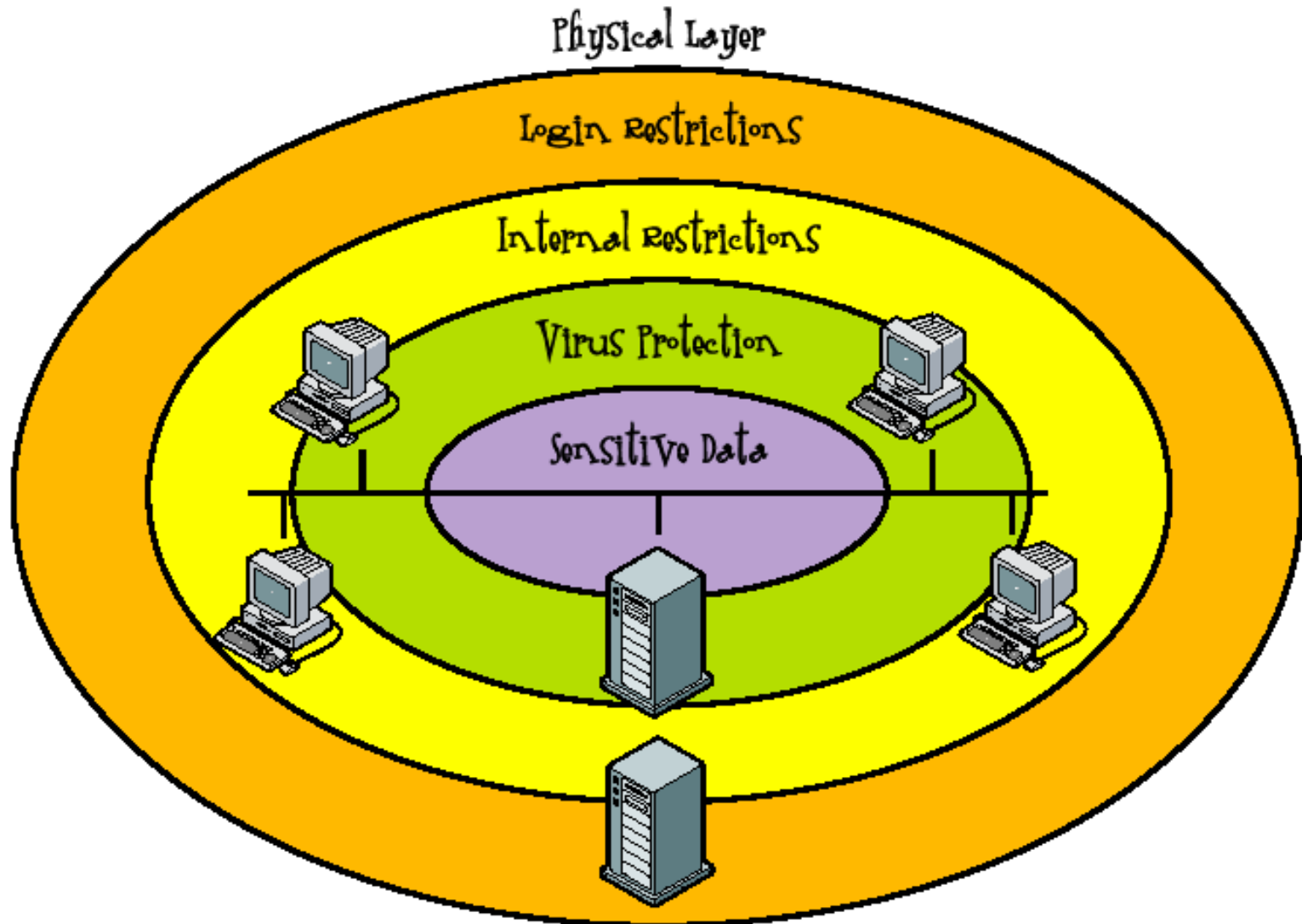
What Virus Protection Should We Use in an Enterprise Network?

- All Workstations should be protected by using Virus protection software
- All Servers should be protected using Virus protection software
- Real-time protection should be enabled on incoming files to protect from infected floppies or viruses coming from the network
- A central server should download and automatically update virus signature patterns on all computers periodically

Digital Immune System



Virus Protection in the Overall Scheme of Things



Computer Security

(Nine rules for data security)

- 1. Establish data security policies
- 2. Establish password management procedures
- 3. Control uploading of programs
- 4. Test new or upgraded software in an isolated computing environment
- 5. Purchase software from reputable sources
- 6. Never leave a network workstation unattended
- 7. Back up data and programs on a regular basis and store them off site
- 8. Establish an effective disaster recovery plan
- 9. Practice "Safe Computing"